L2: Entry 1 of 2   File: JPAB   Jan 23, 1996

PUB-NO: JP408023331A
DOCUMENT-IDENTIFIER: JP 08023331 A
TITLE: METHOD AND DEVICE FOR CIPHERING COMMUNICATION

PUBN-DATE: January 23, 1996

INVENTOR-INFORMATION:
NAME   COUNTRY
MURAKAMI, YASUMICHI
ITO, KAZUHITO

ASSIGNEE-INFORMATION:
NAME   COUNTRY
MURATA MACH LTD

APPL-NO: JP06156307
APPL-DATE: July 7, 1994

INT-CL (IPC): H04 L 9/06; H04 L 9/14; G09 C 1/00; H04 K 1/00

ABSTRACT:

PURPOSE: To attain ciphering and deciphering with simple configuration by applying
self synchronization ciphering to communication information based on a selected
irreducible polynomial, sending the to the received information.

CONSTITUTION: A bit string received by a shift register 15 is subject to arithmetic
operation at prescribed bits while being shifted sequentially therein and the
result is given to an adder 13. The shifting operation is conducted synchronously
with an input operation of the bit string to a terminal 11. That is, the ciphering
is conducted by dividing a message polynomial representing the received bit string
with coefficients in descending order by a ciphering generating polynomial (key).
Then the bit string received from an input terminal 21 is given to an adder 23 and
a primitive polynomial configuration section 24. The adder 23 receives the bit
string from the terminal 21 and the primitive polynomial configuration section 24.
An output of the adder 23 is outputted from a terminal 22 as a decoded bit string.
That is, a decoding circuit 20 uses the same primitive polynomial as that of a
ciphering circuit 10 to decode the ciphered data.